

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

PAIGE THOMPSON,

Defendant.

Case No. CR19-159-RSL

ORDER GRANTING
MOTION TO COMPEL
CAPITAL ONE DATA

This matter comes before the Court on defendant’s “Motion to Compel Capital One Data in the Possession of the Government” (Dkt. # 127). Capital One filed an intervening “Motion Pursuant to 18 U.S.C. § 3771” (Dkt. # 147) asserting that the Crime Victims’ Rights Act (“CVRA”), 18 U.S.C. § 3771, gives it the right to intervene and expressing its objection to defendant’s motion. Defendant further filed a “Motion to File Overlength Reply in Support of Defense Motion to Compel Production of Capital One Data” (Dkt. # 154). Having reviewed the submissions of defendant, the government, and Capital One, and the remainder of the record, the Court finds as follows:

I. Defendant’s Motion to File Overlength Reply

As a threshold matter, the Court grants defendant’s motion to file an overlength reply (Dkt. # 154). Defendant may file a nine-page reply.

II. Capital One's CVRA Motion

The parties dispute whether the Court should consider Capital One's CVRA motion. For the reasons explained below, the Court will consider Capital One's CVRA motion in its analysis of defendant's motion to compel Capital One data.

A. Background

On December 22, 2021, counsel for Capital One filed its "Letter from Aravind Swaminathan" (Dkt. # 130). This letter requested that the Court deny defendant's motion to compel Capital One data, provided a brief supporting argument on the merits, and requested that the Court set a briefing schedule to hear Capital One's arguments. See Dkt. # 130.

On December 31, 2021, without the Court first addressing its letter, Capital One filed its CVRA motion setting forth its arguments in more detail. See Dkt. # 147. On January 10, 2022, the Court granted the parties' "Stipulated Motion to Extend Noting Date" (Dkt. # 157) regarding Capital One's CVRA motion.

B. Propriety of Capital One's CVRA Motion

Capital One argues that the Court has jurisdiction over its CVRA motion because Capital One is a victim under the CVRA, and the CVRA allows crime victims to enforce their rights enumerated in its subsection (a) by filing a motion in the district court where the defendant is being prosecuted. Dkt. # 147 at 5 (citing 18 U.S.C. §§ 3771(d), (e)(2)(A)). Capital One asserts that its motion is to protect its rights enumerated in CVRA subsections (a)(1) and (a)(8), respectively, "to be reasonably protected from the accused," and "to be treated with fairness and with respect for the victim's dignity and privacy." Dkt. # 188 at 2 (quoting 18 U.S.C. §§ 3771(a)(1), (a)(8)).

Defendant counterargues that the Court should strike Capital One's CVRA motion and related letter because (i) the CVRA does not grant Capital One the right to intervene in a pending criminal discovery dispute between the defense and government, but rather grants victims only "the right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding," Dkt. # 172 at 1, 3-4 (quoting 18 U.S.C. § 3771(a)(4)); (ii) the motion was filed without obtaining the Court's prior authorization, ORDER GRANTING MOTION TO COMPEL CAPITAL ONE DATA - 2

1 and the letter makes substantive arguments, Dkt. # 172 at 1, 2-3; and (iii) Capital One's
2 intervention violates defendant's Sixth Amendment rights, Dkt. # 172 at 4.

3 Capital One is correct that the CVRA permits it to file a motion with this Court to assert
4 its rights to be "reasonably protected from the accused" and "treated with fairness and with
5 respect for [its] dignity and privacy." 18 U.S.C. §§ 3771(a)(1), (a)(8), (d)(3). The Ninth Circuit
6 has tacitly recognized that victims may file motions (and petition for writs of mandamus) to
7 enforce CVRA rights, and these enforcement mechanisms are not limited to the right to be heard
8 in public proceedings in the district court involving release, plea, sentencing, or parole. See e.g.,
9 In re K.K., 756 F.3d 1169 (9th Cir. 2014) (reviewing petition for writ of mandamus under the
10 CVRA regarding motions to quash two subpoenas duces tecum); In re Her Majesty the Queen in
11 Right of Canada, 785 F.3d 1273, 1275-77 (9th Cir. 2015) (tacitly recognizing that the CVRA
12 allowed Canada to file a motion for restitution in the district court, to the extent a foreign
13 sovereign could be a CVRA victim).¹ Other district courts have recognized that a victim's right
14 to dignity and privacy as enumerated in subsection (a)(8) of the CVRA includes its interest in
15 preventing disclosure of private information. See, e.g., United States v. Madoff, 626 F. Supp.
16 2d 420, 425-27 (S.D.N.Y. 2009) (applying "dignity and privacy" provision of CVRA to victims'
17 emails); United States v. Bradley, 2011 WL 1102837, at *1 (S.D. Ill. 2011) (finding that
18 subpoenas duces tecum requesting victim's schooling, juvenile court, and mental health records
19 were a "blatant violation" of victim's CVRA right to be treated with respect for his dignity and
20 privacy). Capital One was therefore within its rights to file its CVRA motion.

21 Regarding defendant's second counterargument, defendant points to no authority
22 supporting the proposition that Capital One was required to obtain leave of the Court prior to
23 filing its CVRA motion. Given that the CVRA explicitly authorizes victims to file motions in
24
25

26
27 ¹ The right to restitution is recognized in subsection (a)(6) of the CVRA and is therefore separate
28 from subsection (a)(4)'s right to be heard at public proceedings involving release, plea, sentencing, or
parole. See 18 U.S.C. §§ 3771(a)(4), (6).

1 the district court to assert their rights, see 18 U.S.C. §§ 3771(d)(1), (3), the Court will not strike
2 Capital One's letter and motion on this ground.

3 Regarding defendant's third counterargument, defendant's Sixth Amendment right to
4 confrontation is inapplicable here. The Sixth Amendment's Confrontation Clause provides, "In
5 all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the
6 witnesses against him." U.S. Const. amend. VI. "[T]he principal evil at which the
7 Confrontation Clause was directed was the civil-law mode of criminal procedure, and
8 particularly its use of *ex parte* examinations as evidence against the accused." Crawford v.
9 Washington, 541 U.S. 36, 50 (2004). The Confrontation Clause "applies to 'witnesses' against
10 the accused—in other words, those who 'bear testimony.' 'Testimony,' in turn, is typically 'a
11 solemn declaration or affirmation made for the purpose of establishing or proving some fact.'" Id.
12 at 51 (quoting 2 N. Webster, *An American Dictionary of the English Language* (1828)).
13 Adjudication of this motion does not rest on the Court's resolution of any factual disputes. The
14 Confrontation Clause is therefore not invoked.

15 The Court will therefore consider Capital One's CVRA motion as it looks to the merits of
16 defendant's motion to compel Capital One data.

17 **III. Defendant's Motion to Compel Capital One Data**

18 The Capital One data include the personal identifying information ("PII") of more than
19 100 million Capital One customers, including names, addresses, dates of birth, and, for many
20 fewer individuals, bank account numbers and unencrypted social security numbers. The data
21 were seized from defendant. Dkts. # 145 at 3, # 147 at 1-2, # 155 at 3.

22 Defendant moves to compel disclosure of Capital One data in the government's
23 possession pursuant to Fed. R. Crim. P. 16(a)(1)(E). The government and Capital One both
24 object to defendant's motion and request that the Court exercise its discretion pursuant to Fed.
25 R. Crim. P. 16(d)(1) to conclude that the government need not provide the defense with a copy
26 of the Capital One data.

27 The Court first considers whether defendant has met her burden to obtain production
28 under Fed. R. Crim. P. 16(a)(1)(E), and then considers whether the government or Capital One
ORDER GRANTING MOTION TO COMPEL
CAPITAL ONE DATA - 4

has shown good cause to avoid the requested production of a copy of the data pursuant to Fed. R. Crim. P. 16(d)(1).

A. Fed. R. Crim. P. 16 (a)(1)(E)

Fed. R. Crim. P. 16(a)(1)(E) states:

Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and:²

- (i) the item is material to preparing the defense;
- (ii) the government intends to use the item in its case-in-chief at trial; or
- (iii) the item was obtained from or belongs to the defendant.

Fed. R. Crim. P. 16(a)(1)(E).

The first prong is met because defendant has shown materiality. Materiality is a low threshold; it is satisfied so long as the information would have helped defendant prepare a defense. United States v. Hernandez-Meza, 720 F.3d 760, 768 (9th Cir. 2013) (quoting United States v. Doe, 705 F.3d 1134, 1151 (9th Cir. 2013)). As defendant explains, the Capital One data goes to numerous allegations contained in the indictment, including that (i) the object was "to use the stolen credentials to access and copy other data stored by the customers on Cloud Computing [Company] servers, including data containing valuable personal identifying information," Dkt. # 127 at 4 (quoting Dkt. # 102 at ¶ 11);³ (ii) the data include the PII of approximately 100 million Capital One customers, (iii) the data are valued at over \$5,000;

² It is undisputed that the Capital One data are in the possession of the FBI, and therefore within the government's possession. Dkts. # 127 at 4, # 145 at 1. See United States v. Bryan, 868 F.2d 1032, 1036 (9th Cir. 1989) ("The prosecutor will be deemed to have knowledge of and access to anything in the possession, custody or control of any federal agency participating in the same investigation of the defendant.").

³ Defendant cites to the first superseding indictment (Dkt. # 102), while the second superseding indictment (Dkt. # 166) now controls. However, this allegation is also included in the second superseding indictment. See Dkt. # 166 at ¶ 11.

(iv) defendant attempted to utilize subsets of the data to create counterfeit credit and debit cards; and (v) defendant possessed unlawfully the names and PII of millions of people, Dkt. # 155 at 2 (citing Dkt. # 102 at ¶¶ 19, 24, 32, 34).⁴ That allegations in the indictment rest on the contents of the data is sufficient to show that the data may help defendant to prepare a defense.

The second prong is met because the government acknowledges it will use a subset of the data in its case-in-chief at trial, see Dkt. # 145 at 7, particularly as the defense indicates that the government has failed to identify what this subset will be or provide defendant with such subset, see Dkt. # 155 at 1.

The third prong is met because the data were obtained from the defendant via seizure. This alone entitles the defense to the data.

Capital One argues that the data should be treated as “contraband” and therefore not turned over to the defense despite that the data were seized from the defendant. Dkts. # 147 at 8-9, # 188 at 5-6. In support of this position, Capital One cites to United States v. Benzer, No. 213-CR-00018-JCMGWF, 2015 WL 9200365, at *7 (D. Nev. 2015), United States v. Husband, 246 F. Supp. 2d 467, 469 (E.D. Va. 2003), United States v. Jafari, No. 1:19-0078-SCJ-LTW, 2020 WL 7090698, at *9 (N.D. Ga. 2020), and the definition of “contraband” in Black’s Law Dictionary (11th ed. 2019).

The Court does not find Capital One’s argument to be persuasive. First, none of these sources are binding on this Court. Second, none of these sources compel a conclusion that the data should be made available only for inspection.

The Benzer court considered whether personal and private information previously made available for defense inspection under a protective order should be disclosed to a third-party newspaper, not whether the defense was entitled to the information. See Benzer, 2015 WL 9200365, at *7. Inspection, rather than copying, was stipulated between the government and

⁴ The allegations in list items (ii) through (v) are also included in the second superseding indictment. See Dkt. # 166 at ¶¶ 19, 25, 33, 35.

1 defense. See id. at *1-2. Benzer therefore does not stand for the proposition that the Court
2 should order inspection over the defense's objection.

3 In Husband, the court exercised its discretion under Fed. R. Crim. P. 16(d)(1) and
4 declined to order the government to turn over a tape containing child pornography that it found
5 was contraband subject to forfeiture. Instead, the court allowed the government to arrange
6 inspection without identification of defendant's expert. See Husband, 246 F. Supp. 2d at 469.
7 Child pornography is very different from data such as names, addresses, dates of birth, bank
8 account numbers, and social security numbers, as such data are only made contraband by the
9 method of acquisition and use to which they are put. Further, Husband does not stand for a
10 general proposition that "contraband" cannot be provided in copy to the defense, but rather
11 illustrates that a court may exercise its discretion. Accord United States v. Hill, 322 F. Supp. 2d
12 1081, 1091 (C.D. Cal. 2004), aff'd on other grounds, 459 F.3d 966 (9th Cir. 2006) ("The
13 government argues that since child pornography is contraband, defense counsel and his expert
14 should be required to examine the images in the controlled environment of the government
15 facility. The cases cited by the government, though, all involve appeals from district court
16 decisions denying a defendant's motion to compel production. They do not hold that a district
17 court would abuse its discretion if it were to order the government to produce copies of the
18 materials.").

19 Finally, Jafari concerns a defendant's request for a copy of all data from a third party's
20 cell phone. The Jafari court rejected defendant's conclusory statement that the phone was
21 material to defendant's defense and stated that defendant was required to "point to specific
22 information and demonstrate how that evidence would be relevant to his defense." Jafari, 2020
23 WL 7090698, at *9. This makes sense, given that there was no indication that the third party's
24 cell phone was obtained from the defendant. However, Jafari is inapposite to the case at hand,
25 as it is undisputed that the Capital One data were obtained from the defendant.

26 The Court therefore concludes that defendant is entitled to a copy of the Capital One data
27 pursuant to Fed. R. Crim. P. 16(a)(1)(E).

B. Fed. R. Crim. P. 16 (d)(1)

The government and Capital One argue that the Court should conclude that making the Capital One data available for the defense’s inspection at the FBI’s offices is sufficient to fulfill the government’s Fed. R. Crim. P. 16 obligations. For good cause shown, the Court may “deny, restrict, or defer discovery or inspection, or grant other appropriate relief.” Fed. R. Crim. P. 16(d)(1). The government and Capital One primarily argue that production should be limited (i) in recognition of the privacy interests of the victims, including Capital One and the individuals whose PII is included in the records, and (ii) due to the increased risk of dissemination stemming from allowing the Office of the Federal Public Defenders to possess a copy of the Capital One data.

The Court is sensitive to the victims’ privacy concerns, particularly in light of their rights to be “reasonably protected from the accused” and “treated with fairness and with respect for [their] dignity and privacy” afforded by the CVRA. 18 U.S.C. §§ 3771(a)(1), (a)(8). However, the Court is unpersuaded that restricting the defense team’s access to the Capital One data to the FBI’s office is the correct approach. As was the case in almost every relevant example cited by the government or Capital One, a protective order or redaction (which the government does not offer here) is an appropriate solution that respects the victims’ rights to protection, dignity, and privacy. See, e.g., United States v. Garcia, 625 F.2d 162, 165 (7th Cir. 1980) (redacting prison informant’s name); Haber v. Evans, 268 F. Supp. 2d 507, 512-13 (E.D. Pa. 2003) (in context of third-party access request from newspaper, amending protective order to require redaction of PII of victims, witnesses, confidential informants, and others); United States v. Patkar, Cr. No. 06-00450 JMS, 2008 WL 233062, at *5 (D. Haw. 2008) (in context of third-party access request from Associated Press, upholding protective order preventing disclosure of emails comprising the basis of extortion); United States v. Gatewood, No. CR 11-08074-PCT-JAT, 2012 WL 2286999, at *2 (D. Ariz. 2012) (approving redacted production of victim and witness personal information, particularly given the government’s cooperation with all specific and justified requests); United States v. Jenkins, No. 207CR00080RCJPAL, 2009 WL 10678771, at *2 (D. Nev. 2009) (holding that the government did not have care, custody, or control of the documents

1 and therefore could not produce them, and also noting that the court was not persuaded that
2 defendants were entitled to review the victim's private and sensitive banking records to
3 determine ownership of allegedly defrauded funds); United States v. Dixon, 355 F. Supp. 3d 1,
4 4-9 (D.D.C. 2019) (issuing protective order that allowed defense counsel, but not defendant, to
5 review video footage related to armed robbery); United States v. Torres, No. 20-CR-00418,
6 2020 WL 4500046, at *5 (D.N.J. 2020) (issuing protective order whereby information including
7 sexually explicit images of victims and witnesses would be produced only to defense counsel
8 and not to defendant, and victims' last names would be redacted).

9 Both the government and Capital One rely on United States v. Pac. Gas & Electric Co.,
10 No. 14-CR-00175-TEH, 2015 WL 3958111 (N.D. Cal. 2015), for the proposition that inspection
11 alone is sufficient. The court there found that allowing inspection of the government's witness
12 interview notes and providing the defense copies of only those notes that it intended to use at
13 trial properly balanced the sensitivity of the notes with the defendant's need to have the notes to
14 prepare for trial. However, as the government concedes, Pac. Gas & Electric Co. was decided
15 under Fed. R. Crim. P. 16(a)(1)(B), a provision that explicitly authorizes "inspection, copying,
16 or photographing," Fed. R. Crim. P. 16(a)(1)(B) (emphasis added), while the matter at hand is
17 governed by Fed. R. Crim. P. 16(a)(1)(E), which states that the government must permit the
18 defendant "to inspect *and* to copy or photograph," Fed. R. Crim. P. 16(a)(1)(E) (emphasis
19 added). That the court allowed inspection in Pac. Gas & Electric Co. is therefore unpersuasive,
20 as this was unquestionably in line with the governing rule.

21 In response to Capital One's concerns that defendant herself previously threatened to
22 distribute the data and may do so again, the Court notes that both the government and Capital
23 One protective orders currently in place prevent defendant from accessing the data. Access will
24 be limited to the "Defense Team" as defined in the orders. See Dkts. # 66 (government
25 protective order), # 87 (Capital One protective order).

26 Regarding the increased risk of dissemination, the Court is unpersuaded that this risk is
27 sufficiently grave to merit limiting the defense team's access to the data so long as the data is
28

1 held on a computer that is both not connected to the internet (“air-gapped”) and in a secure
2 location.

3 The Court notes that the article cited by the government regarding the possibility of “Air-
4 Fi” attacks on air-gapped computers states that such attacks are “slow and badly suited for
5 exfiltrating large volumes of data,” such as the Capital One data. The article also indicates that
6 Air-Fi attacks require proximity to the air-gapped computer. See Ben Dickson, ‘Air-Fi’ Attack
7 Renders Air-Gapped Computers Open to Data Exfiltration Through WiFi Signals, The Daily
8 Swig (Dec. 23, 2020, updated June 29, 2021), [https://portswigger.net/daily-swig/air-fi-attack-](https://portswigger.net/daily-swig/air-fi-attack-renders-air-gapped-computers-open-to-data-exfiltration-through-wifi-signals)
9 [renders-air-gapped-computers-open-to-data-exfiltration-through-wifi-signals](https://portswigger.net/daily-swig/air-fi-attack-renders-air-gapped-computers-open-to-data-exfiltration-through-wifi-signals). The government’s
10 concerns regarding “Air-Fi” attacks should be largely addressed by a requirement that the air-
11 gapped computer be held in a secure room.

12 **IV. Conclusion**

13 For all of the foregoing reasons, IT IS HEREBY ORDERED that:

14 1. Defendant’s motion to compel Capital One data (Dkt. # 127) is GRANTED.
15 The government shall immediately provide the defense with one copy of the Capital One data on
16 a hard drive (or other agreed technology) provided to the government by the defense or shall
17 otherwise allow the defense to access the Capital One data at the FBI headquarters and create a
18 copy. The defense shall house the copy of the Capital One data on an air-gapped computer in a
19 secure room at the Federal Public Defender’s Office in Seattle. For the avoidance of doubt, the
20 Capital One data shall be subject to the existing protective orders, including the provision that
21 defendant herself shall not access the Capital One data. See Dkts. # 66, # 87.

22 2. Capital One’s motion pursuant to 18 U.S.C. § 3771 (Dkt. # 147) is DENIED; and

23 3. Defendant’s motion to file overlength reply (Dkt. # 154) is GRANTED.

24 DATED this 21st day of March, 2022.

25
26 

27 Robert S. Lasnik
28 United States District Judge